Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A computer-implemented method for use in ~~a~~ a network environment including an enterprise server, comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between one or more resource servers and a type of security credential required to access each resource server;

receiving at the enterprise server a signal representing a request from ~~a~~ the remote user for a first of the secure ~~resource~~ resources ~~residing on a network employing a generic application layer network protocol~~;

determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource; and

sending from the server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security ~~credential~~ credentials for the user of the type required to access the first secure resource.

Claim 2 (original): The method of claim 1, further comprising:

authenticating the user before sending the signal representing the second request.

Claim 3 (previously presented): The method of claim 1, further comprising:

receiving at the server a signal representing a response to the second request; and

sending from the server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 4 (previously presented): The method of claim 1, wherein the request includes a logon credential for the remote user, the method further comprising: authenticating the remote user based on the logon credential before sending the second request.

Claim 5 (currently amended): The method of claim 1, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, the method further comprising:

sending the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 6 (currently amended): The method of claim 1, wherein the request includes a logon credential for the remote user, the method further comprising:

receiving at the server a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential; and

sending from the server a signal representing the SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the SSO credential.

Claim 7 (currently amended): The method of claim 6, further comprising:

sending from the server a signal representing the SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token.

Claim 8 (currently amended): The method of claim 6, further comprising:

receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

sending from the server a signal representing the second SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the second SSO credential.

Claim 9 (original): The method of claim 1, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 10 (previously presented): The method of claim 9, further comprising:

receiving at the server a signal representing data in response to the second request; and

sending from the server a signal representing at least a portion of the data to the remote user.

Claim 11 (currently amended): The method of claim 10, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 12 (currently amended): The method of claim 1, wherein the receiving includes receiving at the server a signal representing a third request from the remote user for a second of the secure ~~resource~~ resources residing on the network, the method further comprising:

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

sending from the server a signal representing a ~~third~~ fourth request ~~to~~ for retrieving the second secure resource, the ~~third~~ fourth request including a second of the security ~~credential~~ credentials for the user of the type required to access the second secure resource; and wherein the signals representing the second and ~~third~~ fourth requests are sent concurrently.

Claim 13 (currently amended): The method of claim 12, wherein the types of security credentials included in the second and ~~third~~ fourth requests differ.

Claim 14 (currently amended): The method of claim 12, wherein the types of security credentials included in the second and ~~third~~ fourth requests are the same.

Claim 15 (currently amended): The method of claim 1, further comprising:

receiving at the server a signal representing the first security credential from the user before receiving the signal representing the first request.

Claim 16 (cancelled)

Claim 17 (currently amended): An apparatus for use in ~~a~~ a network environment including an enterprise server, comprising:

means for storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

means for maintaining a map between one or more resource servers and a type of security credential required to access each resource server;

means for receiving at the server a signal representing a request from ~~a~~ the remote user for a first of the secure resources ~~resource~~;

means for determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource; and

means for sending from the server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security ~~credential~~ credentials for the user of the type required to access the first secure resource.

Claim 18 (original): The apparatus of claim 17, further comprising:

means for authenticating the user before sending the signal representing the second request.

Claim 19 (previously presented): The apparatus of claim 17, further comprising:

means for receiving at the server a signal representing a response to the second request; and

means for sending from the server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 20 (previously presented): The apparatus of claim 17, wherein the request includes a logon credential for the remote user, the apparatus further comprising:

means for authenticating the remote user based on the logon credential before sending the second request.

Claim 21 (currently amended): The apparatus of claim 17, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, the apparatus further comprising:

means for sending from the server the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 22 (currently amended): The apparatus of claim 17, wherein the request includes a logon credential for the remote user, the apparatus further comprising:

means for receiving at the server a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential; and

means for sending from the server a signal representing the SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the SSO credential.

Claim 23 (currently amended): The apparatus of claim 22, further comprising:

means for sending from the server a signal representing the SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token.

Claim 24 (previously amended): The apparatus of claim 22, further comprising:

means for receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

means for sending from the server a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential.

Claim 25 (original): The apparatus of claim 17, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 26 (previously presented): The apparatus of claim 25, further comprising:

means for receiving at the server a signal representing data in response to the second request; and

means for sending from the server a signal representing at least a portion of the data to the remote user.

Claim 27 (currently amended): The apparatus of claim 26, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 28 (currently amended): The apparatus of claim 17, wherein the means for receiving includes means for receiving at the server a signal representing a

third request from the remote user for a second secure resource residing on the network, the apparatus further comprising:

means for determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

means for sending from the server a signal representing a ~~third~~ fourth request to retrieve the second secure resource, the ~~third~~ fourth request including a second of the security ~~credential~~ credentials for the user of the type required to access the second secure resource; and

wherein the signals representing the second and ~~third~~ fourth requests are sent concurrently.

Claim 29 (currently amended): The apparatus of claim 28, wherein the types of security credentials included in the second and ~~third~~ fourth requests differ.

Claim 30 (currently amended): The apparatus of claim 28, wherein the types of security credentials included in the second and ~~third~~ fourth requests are the same.

Claim 31 (currently amended): The apparatus of claim 17, further comprising:

means for receiving at the server a signal representing the first security credential from the user before receiving the signal representing the first request.

Claim 32 (cancelled)

Claim 33 (currently amended): One or more computer-readable media tangibly embodying a program of instructions executable by a computer to perform a method for use in a network environment including an enterprise server, the method comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between one or more resource servers and a type of security credential required to access each resource server;

receiving at the server a signal representing a request from ~~a~~ the remote user for a first of the secure resources ~~resource residing on a network employing a generic application layer network protocol~~;

determining, by referring to the map and without the intervention of the user, the type of security credential for the remote user that is required to access the first secure resource; and

sending from the server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security ~~credential~~ credentials for the user of the type required to access the first secure resource.

Claim 34 (original): The media of claim 33, wherein the method further comprises:

authenticating the user before sending the signal representing the second request.

Claim 35 (previously presented): The media of claim 33, wherein the method further comprises:

receiving at the server a signal representing a response to the second request; and

sending from the server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 36 (original): The media of claim 33, wherein the request includes a logon credential for the remote user, wherein the method further comprises:

authenticating the remote user based on the logon credential before sending the second request.

Claim 37 (currently amended): The media of claim 33, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, wherein the method further comprises:

sending from the server the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 38 (currently amended): The media of claim 33, wherein the request includes a logon credential for the remote user, wherein the method further comprises:

receiving at the server a signal representing a single-sign-on (SSO) credential generated by a SSO provider based on the logon credential; and

sending from the server a signal representing the SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the SSO credential.

Claim 39 (currently amended) The media of claim 38, wherein the method further comprises:

sending from the server a signal representing the SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO token corresponding to a second SSO provider having a trust relationship with a first SSO provider corresponding to the SSO token.

Claim 40 (currently amended): The media of claim 38, wherein the method further comprises:

receiving at the server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

sending from the server a signal representing the second SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the second SSO credential.

Claim 41 (original): The media of claim 33, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 42 (previously presented): The media of claim 41, wherein the method further comprises:

receiving at the server a signal representing data in response to the second request; and

sending from the server a signal representing at least a portion of the data to the remote user.

Claim 43 (currently amended): The media of claim 42, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 44 (currently amended): The media of claim 33, wherein the receiving includes receiving at the server a signal representing a third request from the remote user for a second secure resource residing on the network, wherein the method further comprises:

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

sending from the server a signal representing a ~~third~~ fourth request ~~to~~ for retrieving the second secure resource, the ~~third~~ fourth request including a second security credential for the user of the type required to access the second secure resource; and

wherein the signals representing the second and ~~third~~ fourth requests are sent concurrently.

Claim 45 (currently amended): The media of claim 44, wherein the types of security credentials included in the second and ~~third~~ fourth requests differ.

Claim 46 (currently amended): The media of claim 44, wherein the types of security credentials included in the second and ~~third~~ fourth requests are the same.

Claim 47 (currently amended): The media of claim 33, wherein the method further comprises:

receiving at the server a signal representing the first security credential from the user before receiving the signal representing the first request.

Claim 48 (cancelled)